Error-Correcting Codes for Multiple-Level Transmission

By JESSIE MacWILLIAMS

(Manuscript received August 2, 1960)

A q-level alphabet is defined as a row vector space over a finite field with q elements. The letters of the alphabet are the rows of the vector space, each consisting of n symbols from the ground field. The weight of a letter is the number of nonzero symbols it contains. The minimum weight of the letters of the alphabet, excluding zero, is denoted by d. A relationship is established between the alphabet and a set of points S in a finite projective space. There is a many-one correspondence between the letters of the alphabet and the hyperplanes of the space. The weight of a letter is simply related to the incidence of the set S with the corresponding hyperplane.

Two sets of points in a finite projective space are called equivalent if they are related by a collineation of the space. Two alphabets are called equivalent if there exists between them, as vector spaces, a weight-preserving semi-isomorphism. It is shown that these definitions mean the same thing and reduce to the usual definition when $q = 2$.

An inequality is established between the dimension of the alphabet and the parameters d, q, n. This gives a lower bound for n in terms of the other parameters. It is shown that this bound cannot be achieved by alphabets with repeated columns. A method is given for constructing a class of alphabets which attain this bound. It is shown that for the case $q = 2$ these are the only alphabets (in the sense of equivalence) for which the bound is attained.

I. INTRODUCTION

A great deal of work has been done on error-correcting codes for the binary channel. In this paper we consider codes for a channel that can transmit more than two levels. Multiple-level transmission is practical if the channel is sufficiently quiet, as, for example, the submarine voice cable. It results in a substantial increase in bit rate and in added flexibility in choosing a code. One now has four parameters to adjust — the number of levels of transmission, the number of information symbols,

the number of redundant symhols, and the numher of errors it is desirable to detect and/or correct. Of course it cannot he decided without detailed analysis whether these advantages will more than compensate for the added complexity of the terminal equipment.

In the binary case, systematic error-correcting codes have certain advantages;[1] in particular, they are amenable to known mathematical techniques. It has heen shown by Slepian[2] that the words of a systematic code form a group under place-by-place addition mod 2. The natural generalization of a group code over the field (0,t) appears to he a vector space over a finite field of q elements. We call such vector spaces *alphabets*, and their individual elements are called *letters*. In the general case, a "code" becomes an "alphabet" and a word (unfortunately!) becomes a "letter." Each letter is a row of n symbols picked from the ground field; the alphabet is a space of row vectors of length n. The q different symhols of the ground field correspond to q different transmission levels.

Because only a restricted type of code is considered, some assumptions must be made ahout the nature of the channel and of the information being transmitted. These are as follows:

(a) The number of transmission levels is a power of a prime number, since the number of elements in a finite field is a power of a prime. In practice this is not a severe restriction; between one and nine we have excluded only the number six.

(b) The channel is "symmetric" in the sense that every symbol has the same chance of getting through correctly, and that the probability of one symbol being changed into another is the same for every pair of symbols.

(c) All errors are equally bad. This might be the case, for example, if one were ordering merchandise from a mail order house by catalog number only.

With these assumptions the principles of error correction by a q-level alphabet are exactly the same as those described by Slepian[2] for a group code (i.e., a two-level alphabet). For convenience, the pertinent results from Slepian's paper are summarized in the Appendix. The parameters of an alphabet, besides n and q are

1. Its dimension as a vector space, denoted hy k. The alphabet contains q^k letters; k is also the number of symbols in each letter which can be regarded as carrying information. The remaining $n - k$ symbols are added for the purpose of error detection and/or correction.

2. The minimum weight, d, of the letters of the alphabet other than $(00 \cdots 0)$. (The weight of a letter is the number of nonzero symbols it contains.) The quantity d is closely related to the error-correcting prop-

erties of the alphabet; if an alphabet is to be capable of correcting all occurrences of $1, 2, \cdots, e$ errors in each letter it must have $d = 2e + 1$.

The purpose of this paper is to investigate the properties of vector spaces over finite fields, particularly those properties which are related to the parameter d. The weight of a letter exists only in relation to a particular base of the vector space, which is an awkward situation in modern algebra. Hence our chief mathematical tool is not algebra but finite projective geometry. The connection between binary group codes and finite geometries was pointed out hy Bose,[3] and is easily extended to the general case.

We first establish several new definitions of equivalence between alphabets. (Two equivalent alphabets have the same error-correcting properties.) A lower hound for n is found in terms of k, q and d. Clearly it is desirahle to have $n - k$ (the number of check symbols) as small as possible. It is shown that tbis lower bound can be attained, but only by a restricted class of alphahets. These alphabets are, on the whole, not practical for communication purposes unless the expected error rate is extremely high. However, the geometric methods used in the construction of these alphabets can be applied to find useful alphabets for specific cases. The theorems derived for q-level alphabets apply equally well to the casc $q = 2$ and contribute to the theory of binary group codes.

II. NOTATION

In this section we define the notation to be used in this paper and introduce Bose's thcorem on the relation between alphabets and projective geometries.†

Let $F(q)$ be a finite field with q elements and characteristic p, and let $F^*(q)$ denote the nonzero elements of $F(q)$. We consider a vector space of dimension n over $F(q)$. Let $G_n(q)$ denote the "row space," i.e., that particular representation of the vector space consisting of all possible n-tuples of elements of $F(q)$. For example, $G_2(4)$ consists of the 2-tuples

$$\begin{array}{cccccc} (00) & (10) & (01) & (11) & (1w) & (1w^2) \\ & (w0) & (0w) & (ww) & (ww^2) & (w1) \\ & (w^20) & (0w^2) & (w^2w^2) & (w^21) & (w^2w) \end{array}$$

where w is a primitive cube root of unity.

Clearly $G_n(q)$ has q^n members. Tbe $q^n - 1$ nonzero elements of $G_n(q)$ can be divided, in many ways, into $(q - 1)$ sets $G_1, \cdots, G_{q-1}$ sucb that $G_i = \lambda G_j$, $\lambda \in F^*(q)$. For our purposes it is usually enough to

† For finite projective geometry, see Carmichael,[4] Ch. 2; for Galois fields, see van der Waerden,[5] Ch. 5, Sect. 37.

examine only one of these sets, for example the first line in the table above.

A subspace of $G_n(q)$ is called an *alphabet over* $F(q)$ and its members are called *letters*. The length of a letter is n and the number of nonzero coordinates in a letter is its weight. Every alphabet contains the letter $(00\cdots0)$. The minimum weight of its other letters is denoted by d, and d is also called the weight of the alphabet. The dimension of the alphabet as a vector space over $F(q)$ is k. By $\mathfrak{A}(k,d,n)$ we mean an alphabet $\mathfrak{A}$ with dimension k, weight d and length (of each letter) n. For example, $G_n(q)$ is $\mathfrak{A}(n,1,n)$.

An alphabet $\mathfrak{A}(k,d,n)$ contains q^k letters, from which we pick any k independent vectors as generators. We write these as the rows of a $k \times n$ matrix $M(\mathfrak{A})$, the *generator matrix* of $\mathfrak{A}$. For example,

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

is the generator matrix of an $\mathfrak{A}(2,2,3)$. We may assume that no column of a generator matrix consists entirely of zeros, for then the alphabet is isomorphic to a subspace of $G_{n-1}(q)$.

An ordered set of k elements of $F(q)$, not all zero (for example, a column of a generator matrix), may be regarded as the coordinates of a point of a projective space $T_{k-1}(q)$, of projective dimension $(k-1)$, over $F(q)$. We shall adopt the convention that a k-tuple which refers to a point of $T_{k-1}(q)$ is to be written as a column vector, e.g.,

$$\mathbf{Q}_1 = \begin{pmatrix} q_{11} \\ q_{21} \\ \vdots \\ q_{k1} \end{pmatrix}.$$

$T_{k-1}(q)$ contains $(q^k-1)/(q-1)$ points; if $\lambda \in F^*(q)$, $\mathbf{Q}$ and $\lambda\mathbf{Q}$ are the same point. The points of $T_{k-1}(q)$ are in one-to-one correspondence with one-dimensional subspaces through the origin in $G_k(q)$.

Let us now write the generator matrix of $\mathfrak{A}(k,d,n)$:

$$M(\mathfrak{A}) = \begin{array}{c} \\ R_1 \\ R_2 \\ \vdots \\ R_k \end{array} \begin{array}{c} \begin{array}{cccc} \mathbf{Q}_1 & \mathbf{Q}_2 & \cdots & \mathbf{Q}_n \end{array} \\ \begin{pmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ q_{k1} & q_{k2} & \cdots & q_{kn} \end{pmatrix} \end{array}$$

and call the rows $R_1, R_2, \cdots, R_k$ and the columns $\mathbf{Q}_1, \mathbf{Q}_2, \cdots, \mathbf{Q}_n$. Regard the columns as a set of points in $T_{k-1}(q)$. There are exactly k independent columns, so this set of points spans the space $T_{k-1}(q)$. Let ν_i be the number of times which some multiple of the column $\mathbf{Q}_i$ [the multiplier being an element of $F^*(q)$] appears in $M(\mathfrak{A})$. The corresponding point in $T_{k-1}(q)$ shall then have multiplicity ν_i. We can now introduce Bose's theorem.†

Theorem 1: Let

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_k \end{pmatrix}$$

be a general point of $T_{k-1}(q)$. Let S denote the set of points $\mathbf{Q}_1, \mathbf{Q}_2, \cdots, \mathbf{Q}_n$ each counted with proper multiplicity. Then the weight of the letter

$$R(\lambda) = \lambda_1 R_1 + \lambda_2 R_2 + \cdots + \lambda_k R_k, \qquad \lambda_i \in F(q)$$

of $\mathfrak{A}$ is equal to the number of points of the set S which do not lie on the hyperplane

$$H(\lambda) \equiv \lambda_1 y_1 + \lambda_2 y_2 + \cdots + \lambda_k y_k = 0$$

of $T_{k-1}(q)$.

Proof: If, for example,

$$\lambda_1 q_{11} + \lambda_2 q_{21} + \cdots + \lambda_k q_{k1} = 0,$$

the point $\mathbf{Q}_1$ lies on $H(\lambda)$. The zeros in the letter $R(\lambda)$ arise from the points of S which lie on $H(\lambda)$, and the number of zeros will be the number of such points counted with proper multiplicity. The weight of $R(\lambda)$ is the number of its nonzero coordinates, which is the number of points of S (again counted with proper multiplicity) not lying on $H(\lambda)$. This proves the theorem.

In Fig. 1, the projective plane $T_2(2)$ is over the field (0,1). Note that $\mathbf{Q}_4\mathbf{Q}_5\mathbf{Q}_6$ are also collinear:

$$\mathbf{Q}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{Q}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{Q}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{Q}_4 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

$$\mathbf{Q}_5 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \mathbf{Q}_6 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{Q}_7 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

† A different proof of this theorem for the field (01) is given in Ref. 3.

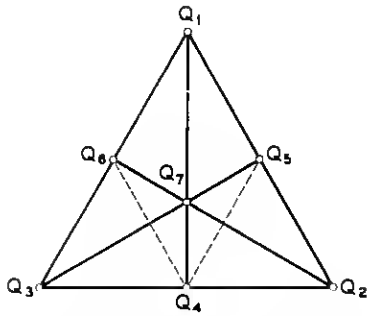

Fig. 1 — Illustration of Theorem 1.

Taking points Q_1, Q_2, Q_3, Q_7 in Fig. 1 as the set N we obtain a generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

of an alphabet $\mathfrak{A}(3,2,4)$. It is clear from the figure that there are at least two points of N not on any line of $T_2(2)$.

III. EQUIVALENT ALPHABETS

In this section we take up the question of equivalent alphabets, and show how Slepian's definition of equivalence may be extended to the more general case. First we discuss what properties one would intuitively hope for from such a definition.

We may consider an alphabet as an array of letters arranged one under another in such a way that we can speak of its columns. We know that the operations of permuting the columns, multiplying any column by an element of $F^*(q)$, and interchanging the names of the nonzero symbols will not change the error-correcting properties of the alphabet. The definition of equivalence between alphabets should allow us to do as many of these things as possible.

From Bose's theorem we recall that the weight of every letter of an alphabet is determined by the properties of a set of points in $T_{k-1}(q)$. First we wish that all alphabets derived from the same set of points should be equivalent; secondly, if two sets of points S, S' have, in some sense, the same incidence relations with the hyperplanes of $T_{k-1}(q)$ they should give rise to equivalent alphabets.

Given a set of points S in $T_{k-1}(q)$, we derive an alphabet from them by means of a generator matrix. We obtain the generator matrix by the following steps:

1. Fix a coordinate system in $T_{k-1}(q)$.†
2. Write the coordinates of the points of S as columns of a matrix repeating each column (not necessarily consecutively) with the proper multiplicity.

The order in which we write the columns is immaterial; also if $\mathbf{X}_i$ is such a column, we have the option of using $\lambda\mathbf{X}_i$, $\lambda \in F^*(q)$, instead. Thus it is apparent that a great many different generator matrices may arise from the same set of points.

We shall presently give separate intrinsic definitions of equivalence between two sets of points, two matrices and two alphabets, and show how they are interrelated. First we give a brief description of the collineation group of $T_{k-1}(q)$.‡

A collineation is a mapping of the set of points of $T_{k-1}(q)$ onto itself which preserves all incidence properties; that is, it sends lines into lines, planes into planes, lines through a point into lines through a point, and so on. The collineations of $T_{k-1}(q)$ form a group, denoted by $C(k,q)$. A nonsingular linear projective transformation of coordinates is a collineation; so is the (nonlinear) transformation of coordinates induced by an automorphism of the ground field $F(q)$. Let $P(k,q)$ be the group of linear projective transformations, and $A(k,q)$ the group of transformations induced by automorphisms of the ground field. Then any collineation of $C(k,q)$ can be expressed as the product of a member of $P(k,q)$ and a member of $A(k,q)$. [Although an element of $P(k,q)$ does not in general commute with an element of $A(k,q)$, the two groups commute as subgroups of $C(k,q)$.] We recall that an automorphism of a finite field of $q = p^m$ elements is always of the form $\theta \rightarrow \theta^{p^\nu}$, where θ is a primitive element; and, for a nontrivial automorphism, $0 < \nu < m$. The integers of the field (the elements of the prime subfield) are not changed by such a mapping; hence a prime field has no nontrivial automorphisms, and in this case $C(k,p) = P(k,p)$.

We now make the following definitions of equivalence:

Definition 1: The (unordered) sets of points S,S' are equivalent if there exists a collineation of $T_{k-1}(q)$ which sends S into S'. We write $S' = C(S)$.

---

† By a fixed coordinate system we mean that the coordinates of every point are fixed, except possibly for multiplication by an element of $F^*(q)$. In the case of finite projective geometries, this involves more than choosing the base points of the system.

‡ The subject is treated in great detail in Carmichael,[4] pp. 355–372.

Definition 2: Two $(k \times n)$ generator matrices M,M' over $F(q)$ are equivalent if

$$M' = g\Phi M^*, \qquad M^* = M\pi\Lambda.$$

Here Φ is an automorphism of the ground field applied to the entries in M^*, g an invertible $(k \times k)$ matrix over $F(q)$, π an $(n \times n)$ permutation matrix, Λ a (nonsingular) diagonal $(n \times n)$ matrix over $F^*(q)$.

Since π has only one nonzero entry in each row and column we can always choose Λ' so that

$$\Lambda'\pi = \pi\Lambda.$$

Definition 3: Two alphabets $\mathfrak{A}$ and $\mathfrak{A}'$ are equivalent if there exists between them a weight-preserving semi-isomorphism.

A semi-isomorphism f between two vector spaces $\mathfrak{A}$, $\mathfrak{A}'$ is uniquely specified by describing what happens to the base vectors $R_1, \cdots, R_k$ of $\mathfrak{A}$, and choosing an automorphism of the ground field. The mapping

$$f(R_i) = R_i', \qquad i = 1, \cdots, k,$$

$$f\left(\sum_{i=1}^{k} \alpha_i R_i\right) = \sum_{i=1}^{k} \Phi(\alpha_i) R_i'$$

is a semi-isomorphism provided that $R_1', \cdots, R_k'$ are linearly independent; any semi-isomorphism can be described in this way.

We note also that a weight-preserving mapping of an alphabet $\mathfrak{A}$ onto an alphabet $\mathfrak{A}'$ is necessarily one-to-one; for only letters of zero weight in $\mathfrak{A}$ can map onto the zero $(00 \cdots 0)$ of $\mathfrak{A}'$.

In all of these definitions, equivalence has its usual properties; i.e., it is symmetric, reflexive and transitive.

We now show that the three definitions are compatible; that is, in a sense to be made precise,

Definition 1 $\rightarrow$ Definition 2,

Definition 2 $\rightarrow$ Definition 3,

Definition 3 $\rightarrow$ Definition 1.

Theorem 2: If S,S' are equivalent in the sense of Definition 1, then the matrices M,M', to which they give rise in a fixed coordinate system, are equivalent in the sense of Definition 2.

Proof: Let $\bar{S}$ be an ordering of the set S, and $\bar{S}'$ the ordering of S'

into which $\bar{S}$ is sent by a collineation $g\Phi$ of $T_{k-1}(q)$. If X_i, X_i' are corresponding points of $\bar{S}, \bar{S}'$ their coordinates are given by

$$\mathbf{X}_i = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad \mathbf{X}_i' = g \begin{pmatrix} \Phi(x_1) \\ \Phi(x_2) \\ \vdots \\ \Phi(x_n) \end{pmatrix}.$$

Let $M(\bar{S})$, $M(\bar{S}')$ denote the matrices with columns

$$\mathbf{X}_1, \cdots, \mathbf{X}_n, \quad \mathbf{X}_1', \cdots, \mathbf{X}_n', \qquad M(\bar{S}') = g\Phi M(\bar{S}).$$

Then there exist permutation matrices such that

$$M'\pi' = M(\bar{S}') = g\Phi M(\bar{S}'), \qquad M(\bar{S}) = M\pi.$$

Hence

$$M' = g\Phi M^*, \quad M^* = M\pi\pi'^{-1} = M\pi^*,$$

where π^* is a permutation matrix.

Theorem 3: If the generator matrices M, M' are equivalent in the sense of Definition 2, then the alphabets $\mathfrak{A}, \mathfrak{A}'$ derived from them are equivalent in the sense of Definition 3.

Proof: We have

$$M' = g\Phi M^*, \qquad M^* = M\pi\Lambda.$$

Let $\mathfrak{A}^*$ be the alphabet derived from M^*. We set up a weight-preserving isomorphism h between $\mathfrak{A}$ and $\mathfrak{A}^*$, and a weight-preserving semi-isomorphism f between $\mathfrak{A}^*$ and $\mathfrak{A}'$. We define h as follows: If R is a letter of $\mathfrak{A}$ then

$$h(R) = R\pi\Lambda.$$

This is clearly a weight-preserving mapping, since its effect is to permute the entries in R and multiply each entry by an element of $F^*(q)$. It is also linear, for if $R_1, \cdots, R_k$ are the rows of M, and $R_1^*, \cdots, R_k^*$ the rows of M^* we have

$$h(R_i) = R_i\pi\Lambda = R_i^*,$$

$$h\left(\sum_{i=1}^{k} \alpha_i R_i\right) = \sum_{i=1}^{k} \alpha_i R_i\pi\Lambda = \sum_{i=1}^{k} \alpha_i R_i^*.$$

We define f as follows: If $R^* = (r_1, r_2, \cdots, r_n)$ is a letter of $\mathfrak{A}^*$, then

$f(R^*) = [\Phi(r_1), \Phi(r_2), \cdots, \Phi(r_n)]$; f is weight-preserving, since $\Phi(r) = 0$ implies $r = 0$.

To show that f is a semi-isomorphism,

$$\mathfrak{A}^* \xrightarrow{f} \mathfrak{A}',$$

we observe that $g^{-1}M'$ is also a generator matrix of $\mathfrak{A}'$. Let $R_1', \cdots, R_k'$ be the rows of $g^{-1}M'$, and let $R_i' = (r_{i1}', r_{i2}', \cdots, r_{in}')$. Let $R_1^*, \cdots, R_k^*$ be the rows of M^*, with $R_i^* = (r_{i1}, {}^*r_{i2}, {}^* \cdots, r_{in}{}^*)$. Since $g^{-1}M' = \Phi M^*$ we have

$$(r_{i1}', r_{i2}', \cdots, r_{in}') = [\Phi(r_{i1}{}^*), \Phi(r_{i2}{}^*), \cdots, \Phi(r_{in}{}^*)],$$

or

$$f(R_i^*) = R_i'.$$

Then

$$f\left(\sum_{i=1}^{k} \alpha_i R_i^*\right) = \left[\Phi\left(\sum_{i=1}^{k} \alpha_i r_{i1}{}^*\right), \Phi\left(\sum_{i=1}^{k} \alpha_i r_{i2}{}^*\right), \cdots, \Phi\left(\sum_{i=1}^{k} \alpha_i r_{in}{}^*\right)\right].$$

Since Φ is a field automorphism this becomes

$$f\left(\sum_{i=1}^{k} \alpha_i R_i^*\right) = \left[\sum_{i=1}^{k} \Phi(\alpha_i)\Phi(r_{i1}{}^*), \sum_{i=1}^{k} \Phi(\alpha_i)\Phi(r_{i2}{}^*), \cdots, \sum_{i=1}^{k} \Phi(\alpha_i)\Phi(r_{in}{}^*)\right]$$

$$= \sum_{i=1}^{k} \Phi(\alpha_i) R_i'.$$

We then have

$$R_i \xrightarrow{h} R_i^* \xrightarrow{f} R_i', \qquad \Sigma\alpha_i R_i \xrightarrow{h} \Sigma\alpha_i R_i^* \xrightarrow{f} \Sigma\Phi(\alpha_i) R_i',$$

and hf is a weight-preserving semi-isomorphism between $\mathfrak{A}$ and $\mathfrak{A}'$.

Theorem 4: Let $\mathfrak{A}, \mathfrak{A}'$ be equivalent alphabets in the sense of Definition 3, and M, M' be any generator matrices of $\mathfrak{A}, \mathfrak{A}'$. Fix the coordinate system in $T_{k-1}(q)$, and let S, S' be the sets of points whose coordinates are the columns of M and M'. Then S and S' are equivalent in the sense of Definition 1.

Lemma: Let the alphabets $\mathfrak{A}, \mathfrak{A}^*$ be related by a weight-preserving isomorphism w; M, M^* are generator matrices of $\mathfrak{A}$ and $\mathfrak{A}^*$ such that $M^* = w(M)$. Then in any coordinate system in $T_{k-1}(q)$ the columns of M and M^* give rise to the same (unordered) set of points S.

Proof of Lemma: If $R_1, \cdots, R_k$; $R_1^*, \cdots, R_k^*$ are the rows of M and M^* we have

$$w(R_i) = R_i^*, \qquad w\left(\sum_{i=1}^{k} \alpha_i R_i\right) = \sum_{i=1}^{k} \alpha_i R_i^*.$$

Let $(y_1 \cdots y_k)$ be the coordinates of the general point of $T_{k-1}(q)$. Map the letters of $\mathfrak{A}$ onto the hyperplanes of $T_{k-1}(q)$ as follows: R_i maps onto $y_i = 0$, $\sum \alpha_i R_i$ maps onto $\sum \alpha_i y_i = 0$. Because of the isomorphism between $\mathfrak{A}$ and $\mathfrak{A}^*$ we have a similar mapping of the letters of $\mathfrak{A}^*$ onto the hyperplanes of $T_{k-1}(q)$: R_i^* maps onto $y_i = 0$, $\sum \alpha_i R_i^*$ maps onto $\sum \alpha_i y_i = 0$.

Let $I = (\delta_{ij})$ be the incidence matrix of points and hyperplanes in $T_{k-1}(q)$, where $\delta_{ij} = 1$ if the ith point lies on the jth hyperplane and is zero otherwise. Each row (column) of I contains $(q^{k-1} - 1)/(q - 1)$ ones and q^{k-1} zeros. The matrix I for the projective plane $T_2(2)$ is illustrated in Table I.

The matrix I is nonsingular. This is easily seen by considering the product $I \cdot I$. In this, all terms on the main diagonal are equal to the number of points, $a = (q^{k-1} - 1)/(q - 1)$, on a hyperplane. All other terms are equal to the number of points, $b = (q^{k-2} - 1)/(q - 1)$, on the intersection of two hyperplanes. The determinant of the matrix is then

$$[a + (\mu - 1)b](a - b)^{\mu - 1}.$$

When we substitute the values for a,b, the first factor becomes

$$\left(\frac{q^{k-1} - 1}{q - 1}\right)^2;$$

hence the determinant is not zero. (We assume $k > 1$.)

Let $P_1, P_2, \cdots, P_\mu$, $\mu = (q^k - 1)/(q - 1)$, be the ordering of the points of $T_{k-1}(q)$ as they appear as columns of I. Let S,S^* be the sets

TABLE I — I = INCIDENCE MATRIX FOR POINTS AND LINES IN $T_2(2)$

	100	010	001	110	101	011	111
$y_1 = 0$	0	1	1	0	0	1	0
$y_2 = 0$	1	0	1	0	1	0	0
$y_3 = 0$	1	1	0	1	0	0	0
$y_1 + y_2 = 0$	0	0	1	1	0	0	1
$y_1 + y_3 = 0$	0	1	0	0	1	0	1
$y_2 + y_3 = 0$	1	0	0	0	0	1	1
$y_1 + y_2 + y_3 = 0$	0	0	0	1	1	1	0

of points whose coordinates are columns of M,M^* respectively. Assign to P_i the multiplicity $n_i(n_i^*)$ with which it appears in the set $S(S^*)$. If P_i does not appear in $S(S^*)$, $n_i = 0$ $(n_i^* = 0)$. Form the column vectors

$$\mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_\mu \end{pmatrix}, \quad \mathbf{n}^* = \begin{pmatrix} n_1^* \\ n_2^* \\ \vdots \\ n_\mu^* \end{pmatrix}.$$

The ith term of the matrix product $I\mathbf{n}$ is the sum of the multiplicities of the points of S which lie on the ith hyperplane. By Theorem 1, this is the number of zeros in the corresponding letters of $\mathfrak{A}$.

Since the isomorphism between $\mathfrak{A}$ and $\mathfrak{A}^*$ is weight-preserving we have

$$I\mathbf{n} = I\mathbf{n}^*,$$

or, since I is invertible,

$$\mathbf{n} = \mathbf{n}^*.$$

Hence the set of points S^* is at most a rearrangement of the set S.

Proof of Theorem 4: $\mathfrak{A}$ and $\mathfrak{A}'$ are related by a weight-preserving semi-isomorphism f. Let $R_1, \cdots, R_k$ be the rows of the generator matrix M of $\mathfrak{A}$. $R_1'' = f(R_1), \cdots, R_k'' = f(R_k)$ are k linearly independent letters of $\mathfrak{A}'$, which we may take as the rows of a generator matrix M'' of $\mathfrak{A}'$. We can describe f as follows:

$$f(R_i) = R_i'', \qquad f\left(\sum_{i=1}^{k} \alpha_i R_i\right) = \sum_{i=1}^{k} \Phi(\alpha_i) R_i'',$$

where Φ is an automorphism of the ground field which is uniquely determined by f once we have chosen M.

Let $R_i^* = \Phi^{-1}(R_i'')$, $i = 1, \cdots, k$; $R_1^*, \cdots, R_k^*$ are linearly independent. Let M^* be the generator matrix formed of these rows and $\mathfrak{A}^*$ the alphabet derived from M^*. The mapping h of $\mathfrak{A}'$ onto $\mathfrak{A}^*$ induced by Φ^{-1} is clearly a weight-preserving semi-isomorphism.

Consider the mapping fh between $\mathfrak{A}$ and $\mathfrak{A}^*$. We have

$$R_i \xrightarrow{f} R_i'' \xrightarrow{h} R_i^*,$$

$$\Sigma\alpha_i R_i \xrightarrow{f} \Sigma\Phi(\alpha_i) R_i'' \xrightarrow{h} \Phi^{-1}[\Sigma\Phi(\alpha_i) R_i''] = \Sigma\alpha_i R_i^*.$$

Since f is weight-preserving by hypothesis, fh is a weight-preserving isomorphism between $\mathfrak{A}$ and $\mathfrak{A}^*$; M and M^* are corresponding generator

matrices under fh, hence by the Lemma they arise from the same set of points S in $T_{k-1}(q)$.

Let S'' be the points of $T_{k-1}(q)$ corresponding to the columns of M''. If

$$\mathbf{X}_i'' = \begin{pmatrix} x_1'' \\ \vdots \\ x_k'' \end{pmatrix}, \quad \mathbf{X}_i{}^* = \begin{pmatrix} x_1{}^* \\ \vdots \\ x_k{}^* \end{pmatrix}$$

are the ith columns of M'' and M^* respectively, we have

$$\begin{pmatrix} x_1'' \\ \vdots \\ x_k'' \end{pmatrix} = \begin{pmatrix} \Phi(x_1{}^*) \\ \vdots \\ \Phi(x_k{}^*) \end{pmatrix}.$$

Hence the set S'' is obtained from the set S^* by a collineation C_1 of $T_{k-1}(q)$.

Let M' be any generator matrix of $\mathfrak{C}'$; then $M' = gM''$. Let S' be the points of $T_{k-1}(q)$ corresponding to the columns of M'. S' arises from S'' by a linear projective transformation, i.e., by a collineation C_2.

We have then

$$S' = C_2(S'') = C_2C_1(S),$$

which proves the theorem.

It can be shown from Theorems 2, 3 and 4 that a complete equivalence class of sets of points gives rise to a complete equivalence class of matrices; a complete equivalence class of matrices gives rise to a complete equivalence class of alphabets; and this in turn gives rise to a complete equivalence class of sets of points. The details of these correspondences are quite complicated, since an unordered set of points can give rise to many matrices, and different generator matrices can produce the same alphabet.

Theorems 2, 3 and 4 are, of course, true over the field (0,1). We rewrite our definitions for this field, since they take a simpler form. Φ is the identity, and the only possible choice for Λ is the unit matrix.

Definition 1': Two sets of points S,S' in $T_{k-1}(2)$ are equivalent if they are related by a linear projective transformation of coordinates.

Definition 2': Two $(k \times n)$ matrices M,M' over $F(2)$ are equivalent if

$$M = gM'\pi,$$

where π is an $(n \times n)$ permutation matrix, and g an invertible $(k \times k)$ matrix over $F(2)$.

Definition 3': Two alphabets $\mathfrak{A},\mathfrak{A}'$ over $F(2)$ are equivalent if they are isomorphic as groups in such a way that corresponding elements have the same weight.

It will be recognized that this is, in fact, the familiar definition of equivalence for alphabets over (0,1).

IV. RELATIONS BETWEEN k, d, n

In this section we establish certain relations between the parameters k,d,n, which are necessary conditions for the existence of an alphabet $\mathfrak{A}(k,d,n)$. We assume, as before, that the alphabet has no column consisting entirely of zeros.

Define $Z[x]$ to mean the least integer greater than or equal to the rational number x.

Theorem 5:† A necessary condition for the existence of $\mathfrak{A}(k,d,n)$ is that

$$n \geqq Z\left[\frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)d\right].$$

Proof: As before, let I be the incidence matrix of points and hyperplanes in $T_{k-1}(q)$.

Let J be the complement of I obtained by replacing zeros by ones and ones by zeros. J is symmetric; each row (column) contains q^{k-1} ones and $1 + q + \cdots + q^{k-2}$ zeros.

The matrix J for the projective plane $T_2(2)$ over the field (0,1) is illustrated in Table II.

Let

$$\mathbf{n} = \begin{bmatrix} n_1 \\ n_2 \\ \vdots \\ n_\mu \end{bmatrix},$$

where $\mu = 1 + q + \cdots + q^{k-1}$ and n_i stands for the multiplicity of the point P_i of $T_{k-1}(q)$.

Consider the expression $J\mathbf{n}$. The product of the ith row of J with the column of n_i is the sum of the multiplicities of the points P_i which do not lie on the ith hyperplane. By Bose's theorem, this is the weight of the letters of the alphabet corresponding to the ith hyperplane. Now

† This theorem has been obtained for the field (0,1) by many authors in as many ways. See for example, Ref. 6, Theorem 5; Ref. 3, Eq. (52), and other authors quoted in Ref. 3.

TABLE II — J = COMPLEMENT OF I

	100	010	001	110	101	011	111
$y_1 = 0$	1	0	0	1	1	0	1
$y_2 = 0$	0	1	0	1	0	1	1
$y_3 = 0$	0	0	1	0	1	1	1
$y_1 + y_2 = 0$	1	1	0	0	1	1	0
$y_1 + y_3 = 0$	1	0	1	1	0	1	0
$y_2 + y_3 = 0$	0	1	1	1	1	0	0
$y_1 + y_2 + y_3 = 0$	1	1	1	0	0	0	1

define a column vector

$$\mathbf{d} = \begin{pmatrix} d \\ d \\ \vdots \\ d \end{pmatrix}.$$

Since our alphabet is assumed to have minimum weight d, we have the inequalities

$$J\mathbf{n} \geqq \mathbf{d}.$$

Since we may assume $d \geqq 1$, these inequalities imply that there must be at least one point of nonzero multiplicity not lying on any given hyperplane — that is, the points of nonzero multiplicity span the space $T_{k-1}(q)$.

Hence, given k and d, the least value of n for which there exists an alphabet $\mathfrak{A}(k,d,n)$ is the minimum value of

$$\sum_{i=1}^{\mu} n_i ,$$

where n_i, $i = 1, \cdots, \mu$ are nonnegative integers which satisfy $J\mathbf{n} \geqq \mathbf{d}$.

By adding all the inequalities of $J\mathbf{n} \geqq \mathbf{d}$, we obtain

$$q^{k-1} \sum_{i=1}^{\mu} n_i \geqq (1 + q + \cdots + q^{k-1})\, d,$$

or, setting

$$n = \sum_{i=1}^{\mu} n_i ,$$

$$n \geqq Z\left[\frac{1}{q^{k-1}}\left(\frac{q^k - 1}{q - 1}\right) d\right].$$

In the case that $d = q^{k-1}$, for any value of k the lower bound becomes

$$n \geqq \frac{q^k - 1}{q - 1} = 1 + q + \cdots + q^{k-1}.$$

In this case the lower bound is the largest possible lower bound, as it is achieved by the alphabet which corresponds to $n_1 = n_2 = \cdots = n_\mu = 1$, that is, the alphabet which results from taking every point of $T_{k-1}(q)$ with multiplicity one.

One has an intuitive feeling that alphabets with the least n for a given k,d are likely to have no repeated columns if this is possible. This is partly justified by the following theorem.

Theorem 6: If a generator matrix of $\mathfrak{A}(k,d,n)$ contains a repeated column [in the sense that $\mathbf{Q}_i = \lambda \mathbf{Q}_s$ for some λ of $F^*(q)$], then

$$n \geqq Z\left[\frac{1}{q^{k-2}}\left(\frac{q^{k-1} - 1}{q - 1}\right) d\right] + 2.$$

For the purposes of this proof and the succeeding lemma we write the above inequality as

$$n \geqq Z\left[\frac{q}{q - 1}\left(1 - \frac{1}{q^{k-1}}\right) d\right] + 2.$$

Proof: Let P be the point of $T_{k-1}(q)$ which corresponds to the repeated column. Choose a coordinate system in which P is one of the base points, say $P = \mathbf{e}_1$. We then have an equivalent alphabet $\mathfrak{A}'$ which may be written

$$M(\mathfrak{A}') = \left(\begin{array}{ccccc|c} 1 & 1 & 0 & \cdots & 0 & \cdots \\ 0 & 0 & 1 & \cdots & 0 & \cdots \\ \vdots & \vdots & \vdots & & & \\ 0 & 0 & 0 & \cdots & 1 & \cdots \end{array}\right).$$

The letters of $\mathfrak{A}'$ to which the first two columns contribute zeros form a vector space $\overline{\mathfrak{A}}$; $\overline{\mathfrak{A}}$ is generated by the rows $2, \cdots, k$ of $M(\mathfrak{A}')$. The minimum weight of the letters of $\overline{\mathfrak{A}}$ is at least as great as the minimum weight of the letters of $\mathfrak{A}'$. Hence the alphabet $\overline{\mathfrak{A}}$ has parameters $k - 1$, d', $n - 2$, with $d' \geqq d$. By Theorem 3 we get

$$n - 2 \geqq Z\left[\frac{q}{q - 1}\left(1 - \frac{1}{q^{k-1}}\right) d'\right],$$

or

$$n \geqq Z\left[\frac{q}{q - 1}\left(1 - \frac{1}{q^{k-1}}\right) d\right] + 2.$$

It is clear that, if $d \leqq 2q^{k-1}$

$$\frac{q}{q-1}\left(1-\frac{1}{q^{k-1}}\right)d+2 \geqq \frac{q}{q-1}\left(1-\frac{1}{q^k}\right)d.$$

We need a little more, namely:

Lemma: If $d \leqq q^{k-1}$, then

$$\frac{q}{q-1}\left(1-\frac{1}{q^{k-1}}\right)d+2 \geqq \frac{q}{q-1}\left(1-\frac{1}{q^k}\right)d+1.$$

Hence

$$Z\left[\frac{q}{q-1}\left(1-\frac{1}{q^{k-1}}\right)d+2\right] > Z\left[\frac{q}{q-1}\left(1-\frac{1}{q^k}\right)d\right].$$

Proof:

$$\begin{aligned}\frac{q}{q-1}\left(1-\frac{1}{q^{k-1}}\right)d+2 &= \left[\frac{q}{q-1}\left(1-\frac{1}{q^k}\right)\right.\\ &\qquad \left.+\frac{q}{q-1}\left(\frac{1}{q^k}-\frac{1}{q^{k-1}}\right)\right]d+2\\ &= \frac{q}{q-1}\left(1-\frac{1}{q^k}\right)d-\frac{d}{q^{k-1}}+2\\ &\geqq \frac{q}{q-1}\left(1-\frac{1}{q^k}\right)d+1.\end{aligned}$$

Theorem 7: If $d \leqq q^{k-1}$ the bound given in Theorem 3 cannot be attained by an alphabet with repeated columns.

Tbis result is not surprising in view of tbe remark at the end of the proof of Theorem 3. If $d > q^{k-1}$, the inequality of Theorem 5 gives $n > (q^k-1)/(q-1)$; i.e., n is larger than the total number of points in the space $T_{k-1}(q)$. Thus we must have repeated columns in the generator matrix.

By repeated applications of the procedure of Theorem 6 we can write down lower bounds for the n of alphabets having a given number of columns with given multiplicities. However, this does not seem very interesting; we will first say what we can about alphabets with no repeated columns. We assume from now on that we are dealing witb such alpbabets.

V. A CLASS OF ALPHABETS

In this section we describe a class of alphabets for which the bound of Theorem 5 is attained, and show how other alphabets which attain this bound may be derived from them.

We can immediately write down the class of alphabets.† Choose a fixed k, and consider the following sets of points in $T_{k-1}(q)$:

(0) — The set S_0 of all points of $T_{k-1}(q)$:

$$n_0 = 1 + q + \cdots + q^{k-1}, \qquad d_0 = q^{k-1}.$$

Every letter of this alphabet has weight d_0.

(1) — The set S_1 of all points but one of $T_{k-1}(q)$:

$$n_1 = q + q^2 + \cdots + q^{k-1}, \qquad d_1 = q^{k-1} - 1.$$

The $(1 + q + \cdots + q^{k-2})$ hyperplanes through the omitted point correspond to letters of weight q^{k-1}, other hyperplanes to letters of weight $q^{k-1} - 1$.

(2) — S_2 = all points of $T_{k-1}(q)$ except for the $(1 + q)$ points of a line L_1.

$$n_2 = q^2 + \cdots + q^{k-1}, \qquad d_2 = q^{k-1} - q.$$

The $(1 + q + \cdots + q^{k-3})$ hyperplanes through L_1 correspond to letters of weight q^{k-1}, others to letters of weight $q^{k-1} - q$.

(3) — S_3 = all points of $T_{k-1}(q)$ except for the $(1 + q + q^2)$ points of a plane P_2.

$$n_3 = q^3 + \cdots + q^{k-1}, \qquad d_3 = q^{k-1} - q^2.$$

The $(1 + q + \cdots + q^{k-4})$ hyperplanes through P_2 correspond to letters of weight q^{k-1}, other hyperplanes to letters of weight $q^{k-1} - q^2$.

.
.
.

$(k - 1)$ — S_{k-1} = all points of $T_{k-1}(q)$ except for the points of a hyperplane

$$n_{k-1} = q^{k-1}, \qquad d_{k-1} = q^{k-1} - q^{k-2}.$$

The omitted hyperplane corresponds to letters of weight q^{k-1}, all others to letters of weight $q^{k-1} - q^{k-2}$.

It is easy to verify that for these alphabets the bound of Theorem 3 is attained. Consider

---

† For the case of $q = 2$ some, or all, of these alphabets have been found by other authors by different methods. See, for example, Refs. 3 and 6. They are, of course, picked up by any systematic search, such as linear programming. $\mathfrak{A}_{k-1}$ is the Reed-Muller code for $m = n$, $r = 1$.

$$n_i - \frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)d_i = q^i + \cdots + q^{k-1} - \frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)(q^{k-1} - q^{i-1})$$

$$= q^i\left(\frac{q^{k-i}-1}{q-1}\right) - \frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)(q^{k-i}-1)q^{i-1}$$

$$= \frac{q^{k-i}-1}{q-1}\left(q^i - \frac{q^k-1}{q^{k-i}}\right)$$

$$= \frac{1}{q^{k-i}}\left(\frac{q^{k-i}-1}{q-1}\right).$$

Since $q \geqq 2$, this quantity is less than one; i.e.,

$$1 > n_i - \frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)d_i > 0.$$

It will appear presently that for $q = 2$ these are the only alphabets which attain the bound of Theorem 5. The case $q > 2$ is more complicated.

Suppose that $\mathfrak{A}(k,d,n)$ is an alphabet (with no repeated columns) for which

$$n = Z\left[\frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right)d\right].$$

Write

$$\frac{1}{q^{k-1}}\left(\frac{q^k-1}{q-1}\right) = 1 + \frac{Q}{q^{k-1}}, \qquad Q = q^{k-2} + \cdots + q + 1 = \frac{q^{k-1}-1}{q-1},$$

$$n = Z\left[d + \frac{Qd}{q^{k-1}}\right].$$

Let

$$Qd = sq^{k-1} - r, \qquad 0 \leqq r \leqq q^{k-1} - 1, \qquad 0 < s \leqq Q, \qquad (1)$$

where r and s are integers; s cannot be zero since d is positive; $s \leqq Q$ since $d \leqq q^{k-1}$. Then

$$n = Z\left[d + s - \frac{r}{q^{k-1}}\right] = d + s.$$

If we remove η columns from the generator matrix of $\mathfrak{A}$ in such a way that the remaining matrix is of rank k (this is always possible for $\eta \leqq n - k$), we obtain an alphabet of length $n - \eta$ and minimum weight $\bar{d} \geqq d - \eta$. Let us consider the worst case, i.e., $\bar{d} = d - \eta$.

Lemma: If

$$n = Z\left[\frac{1}{q^{k-1}}\left(\frac{q^k - 1}{q - 1}\right) d\right],$$

then

$$n - \eta = Z\left[\frac{1}{q^{k-1}}\left(\frac{q^k - 1}{q - 1}\right)(d - \eta)\right]$$

provided that

$$\eta < (q - 1) - \frac{q - 1}{q^{k-1} - 1}(r - 1). \tag{2}$$

Proof:

$$Z\left[\left(1 + \frac{Q}{q^{k-1}}\right)(d - \eta)\right] = Z\left[d + s - \frac{r}{q^{k-1}} - \eta - \frac{\eta Q}{q^{k-1}}\right]$$

$$= Z\left[(d + s - \eta) - \frac{Q\eta + r}{q^{k-1}}\right].$$

This is equal to $d + s - \eta$ if and only if $(Q\eta + r)/q^{k-1} < 1$; i.e.,

$$\eta < \frac{1}{Q}(q^{k-1} - r) = (q - 1)\frac{q^{k-1}}{q^{k-1} - 1} - (q - 1)\frac{r}{q^{k-1} - 1}$$

or

$$\eta < (q - 1) - (q - 1)\frac{r - 1}{q^{k-1} - 1}.$$

Now suppose that $\bar{d} > d - \eta$, and η satisfies (2):

$$Z\left[\left(1 + \frac{Q}{q^{k-1}}\right)\bar{d}\right] \geqq Z\left[\left(1 + \frac{Q}{q^{k-1}}\right)(d - \eta)\right] = n - \eta.$$

By Theorem 3 applied to the alphabet $\mathfrak{A}(k,\bar{d},n - \eta)$, we have

$$n - \eta \geqq Z\left[\left(1 + \frac{Q}{q^{k-1}}\right)\bar{d}\right].$$

Hence only equality is possible.

Theorem 8: If $\mathfrak{A}(k,d,n)$ attains the bound of Theorem 5 and $\mathfrak{A}(k,d,n - \eta)$ is obtained from it by removing η columns from a generator matrix of $\mathfrak{A}$, where η satisfies (2) in such a way that the remaining matrix is of rank k, then the new alphabet also attains the bound of Theorem 5.

We remark that if we select the columns with proper care, it is possible to remove more than the number given by (2) and still obtain an alphabet which attains the bound of Theorem 5. The alphabets $\mathfrak{A}_2, \cdots, \mathfrak{A}_{k-1}$ listed at the beginning of this section are examples.

We now reformulate (2) in a more convenient form. We observe, from (1), that, since d is an integer, so is $(sq^{k-1} - r)/Q$. Subtract from it the integer

$$s(q-1) - \frac{s(q^{k-1}-1)}{Q}$$

and we find that

$$\frac{s-r}{Q} = \frac{s-r}{q^{k-2} + \cdots + q + 1}$$

is also an integer. We have two cases:

i. $s = Q, r = \mu Q \qquad [\mu \leqq q-1$ from (1)].

Then (2) becomes

$$\eta < (q-1) - \mu + \frac{1}{Q}$$

or, since all these symbols represent integers,

$$\eta \leqq (q-1) - \mu. \tag{3}$$

ii. $s < Q, r = \mu Q + s \qquad \left[\mu < \left(1 - \frac{s}{q^{k-1}-1}\right)(q-1) \text{ from (1)}\right].$

Then (2) becomes

$$\eta < (q-1) - \mu - \frac{s-1}{Q}$$

or

$$\eta \leqq q - 1 - \mu - 1 = q - 2 - \mu. \tag{4}$$

In case i we have, from (1),

$$d = q^{k-1} - \mu, \qquad 0 \leqq \mu \leqq q-1.$$

The alphabet $\mathfrak{A}_0$ corresponds to the case $\mu = 0$, and the alphabet $\mathfrak{A}_1$ to $\mu = 1$. From the alphabet $\mathfrak{A}_0$ we can subtract any number $\eta \leqq q-1$ of columns and obtain an alphabet which attains the bound of Theorem 5. (The alphabet $\mathfrak{A}_1$ is obtained by subtracting one arbitrary column.)

In case ii we have, from (1),

$$d = \frac{sq^{k-1}}{Q} - \frac{\mu Q + s}{Q} = s(q-1) - \mu.$$

For the alphabets $\mathfrak{A}_2, \cdots, \mathfrak{A}_{k-1}$ we have $\mu = 0$. This is readily verified by direct calculation:

$$d_i = q^{k-1} - q^{i-1} = q^{i-1}(q^{k-i} - 1) = (q-1)q^{i-1}(q^{k-i-1} + \cdots + q + 1).$$

Thus

$$s = (q^{k-2} + \cdots + q^{i-1}), \qquad \mu = 0.$$

We shall show that these are the only alphabets besides $\mathfrak{A}_0$ for which $\mu = 0$.

The generator matrix of an alphabet $\mathfrak{A}(k,d,n)$ with no repeated columns consists of a subset of the columns of the generator matrix $M(\mathfrak{A}_0)$. Let S be the generating points of $\mathfrak{A}(k,d,n)$ in $T_{k-1}(q)$, and denote by $C(S)$ the points of $T_{k-1}(q)$ which are not in S.

Let ν be the number of points in $C(S)$ and δ the *maximum* number of points of $C(S)$ which do not lie on a hyperplane of $T_{k-1}(q)$. The alphabet $\mathfrak{A}$ then has length $n_0 - \nu$ and weight $d_0 - \delta$, where $n_0 = (q^k - 1)/(q-1)$, $d_0 = q^{k-1}$ are the parameters of $\mathfrak{A}_0$. Using Theorem 5 on these numbers, we obtain

$$\left(\frac{q^k - 1}{q-1} - \nu\right)(q-1) \geqq \frac{q^k - 1}{q^{k-1}}(q^{k-1} - \delta),$$

or

$$\nu(q-1) \leqq \left(q - \frac{1}{q^{k-1}}\right)\delta.$$

Since $\nu(q-1)$ is an integer we may replace this by

$$\nu(q-1) \leqq q\delta - 1. \tag{5}$$

This is the best we can do, since $\delta \leqq q^{k-1}$.

By some further manipulation we find that for the alphabet a, generated by $\mathfrak{A}_0 - C(S)$, to attain the bound of Theorem 5 we must have

$$(q\delta - 1) - (q-2) \leqq \nu(q-1) \leqq q\delta - 1. \tag{6}$$

We also wish to have an alphabet with $\mu = 0$; for such an alphabet

$$d = \frac{sq^{k-1} - s}{Q} = s(q-1),$$

$$\delta = d_0 - d = q^{k-1} - s(q-1),$$

$$q\delta - 1 = (q^k - 1) - sq(q-1);$$

i.e., $q\delta - 1$ is divisible by $(q - 1)$. From (6), the only possibility is

$$\nu(q - 1) = q\delta - 1. \tag{7}$$

We also observe from (6) that if $q = 2$ we have $\nu(q - 1) = q\delta - 1$ without any other considerations.

To justify our statement that $\mathfrak{A}_2, \cdots, \mathfrak{A}_{k-1}$ are the only alphabets besides $\mathfrak{A}_0$ for which $\mu = 0$, we prove the following theorem.

Theorem 9: If $C(S)$ is a set of ν points in $T_{k-1}(q)$, with δ defined as above, and $\nu(q - 1) = q\delta - 1$, then $C(S)$ is the set of all points of a linear space in $T_{k-1}(q)$. This, of course, implies that

$$\nu = 1 + q + \cdots + q^s, \qquad \delta = q^s, \qquad 1 \leqq s \leqq k - 2.$$

Conversely, if $C(S)$ is the set of all points of a linear space, then the alphabet $\mathfrak{A}$ has $\mu = 0$ and attains the bound of Theorem 5. This we have already verified.

Proof: We have $\nu - \delta = (\nu - 1)/q$, so that $(\nu - 1)$ must be a multiple of q. If $\nu = 1$ the corresponding alphabet is $\mathfrak{A}_1$, for which $\mu = 1$.

The proof is by induction on δ; we start by proving the theorem for the case $(\nu - 1)/q = 1$; i.e., $\delta = q$, $\nu = q + 1$.

Lemma: If $\nu = 1 + q$ and $\delta = q$, the $(1 + q)$ points $X_0, X_1, \cdots, X_q$ are collinear, however large the containing space.

An equivalent statement, which is the one we prove, is: If every hyperplane of $T_{k-1}(q)$ contains at least one of the points $X_0, X_1, \cdots, X_q$, then $X_0, X_1, \cdots, X_q$ are the points of a line.

We may assume that there is one hyperplane, say $Y_1 = 0$, which contains exactly one point X_i, which we may call X_1. Pick another point for X_0 and let the coordinates of these two points be $\mathbf{e}_1, \mathbf{e}_2$. We assume the coordinate system normalized so that the first nonzero coordinate of every point is unity. Write the coordinates of the X_i as columns of a matrix as follows:

$$\begin{array}{c} \\ Y_1 \\ Y_2 \\ Y_3 \\ \vdots \\ Y_k \end{array} \begin{array}{c} \begin{array}{cccccc} \mathbf{X_0} & \mathbf{X_1} & \mathbf{X_2} & \mathbf{X_3} & \cdots & \mathbf{X_q} \end{array} \\ \left[\begin{array}{cccccc} 1 & 0 & 1 & 1 & \cdots & 1 \\ 0 & 1 & a_2 & a_3 & \cdots & a_q \\ 0 & 0 & b_2 & b_3 & \cdots & b_q \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & f_2 & f_3 & \cdots & f_q \end{array}\right] \end{array}.$$

By Theorem 1, every letter of the form $\alpha Y_1 + \beta Y_2$ must contain at least one zero coordinate. For $\alpha = 0$ $(\beta = 0)$ we always have a zero in the

second (first) place of such a letter. In the $(q-1)$ letters of the form $\alpha Y_1 + Y_2$, $\alpha \in F^*(q)$, the zero must occur in one of the places $2, 3, \cdots, q$. Hence the $a_2, a_3, \cdots, a_q$ above must denote some arrangement of all the elements of $F^*(q)$.

Consider now letters of the form

$$\alpha Y_1 + \beta Y_2 + \gamma Y_3 .$$

Again, the first two coordinate places take care of those letters for which one of α,β,γ is zero. Hence we restrict ourselves to letters

$$\alpha Y_1 + \beta Y_2 + Y_3 , \qquad \alpha,\beta \in F^*(q).$$

Each such letter must have a zero in one of the places $2, 3, \cdots, q$.

We note that there are $(q-1)^2$ such letters, and $(q-1)$ coordinate places.

Suppose now that $b_2 \neq 0$. We shall count the number of letters to which the $\mathbf{X}_2$ column contributes a zero. We may choose any α in $F^*(q)$ such that $\alpha \neq b_2$. $\beta(\neq 0)$ is then uniquely determined by the equation [in $F(q)$]

$$\beta a_2 = -(\alpha + b_2).$$

Hence if $b_2 \neq 0$ the $\mathbf{X}_2$ column contributes a zero to only $(q-2)$ letters.

If $b_2 = 0$ we have $(q-1)$ choices for α, and β is determined by

$$\beta a_2 = -\alpha.$$

In this case the $\mathbf{X}_2$ column contributes a zero to $(q-1)$ letters.

Hence the only possible choice for b_i is $b_i = 0$ for all i.

The same argument shows that all rows Y_i, $i > 3$, consist entirely of zeros. The coordinates of $X_2, \cdots, X_q$ are linearly dependent on those of X_0,X_1; that is, the points $X_2, \cdots, X_q$ all lie on the line joining X_0,X_1.

Returning now to the main theorem we make the following induction hypothesis:

Let $C(S)$ be a set of ν points in $T_{k-1}(q)$, with δ defined as before, and such that

$$(q-1)\nu = q\delta - 1. \tag{7}$$

Let $q^{r-2} < \delta \leqq q^{r-1}$, and assume that Theorem 9 is true for values of $\delta \leqq q^{r-2}$. We wish to prove that

i. $\delta = q^{r-1}$, $\qquad \nu = 1 + q + q^2 + \cdots + q^{r-1}$.

ii. $C(S)$ consists of all points of a linear space of projective dimension $(r-1)$.

From (7), $\nu - \delta = (\nu - 1)/q = h$, where h is an integer greater than 1. $h = 1$ is the case already considered in the Lemma. Also

$$\delta = \nu - h = hq + 1 - h.$$

An arbitrary space of dimension $(k - 3)$, say D_{k-3}, in $T_{k-1}(q)$ will contain a number α of points of $C(S)$. We wish to find a lower bound $\bar{\alpha}$ for α.

There are $(q + 1)$ hyperplanes of $T_{k-1}(q)$ which pass through D_{k-3}. Denote by $\beta_0, \beta_1, \cdots, \beta_q$ the number of points of $C(S)$, outside of D_{k-3}, contained by these hyperplanes. The hyperplanes through D_{k-3} contain among them all points of $T_{k-1}(q)$, so certainly all of $C(S)$. We have then

$$\begin{aligned} \alpha + \sum_{i=0}^{q} \beta_i &= \nu = hq + 1, \\ \alpha + \beta_i &\geqq \nu - \delta = h. \end{aligned} \tag{8}$$

A lower bound for α is obtained by making all the β_i equal, $\beta_i = \bar{\beta}$, and replacing "$\geqq$" by "$=$" in (8). Then,

$$\bar{\alpha} + \bar{\beta} = h,$$

$$\bar{\alpha} + (q + 1)\bar{\beta} = hq + 1.$$

Solving these equations,

$$\bar{\alpha} = \frac{h - 1}{q}.$$

$$\bar{\beta} = h - \frac{h - 1}{q} = \frac{\delta}{q}.$$

Let α' be the least integer containing $\bar{\alpha}$. We note that $\alpha' > 0$.

We may assume that some hyperplane, say H_{k-2}, of $T_{k-1}(q)$ contains exactly $\nu - \delta = h$ points of $C(S)$. Call this set of points $C(S')$. Each hyperplane of H_{k-2} is a $(k - 3)$-dimensional subspace of $T_{k-1}(q)$, and so by the previous result it contains at least α' points of $C(S')$.

For $C(S')$ we have

$$\nu' = h, \qquad \delta' \leqq h - \alpha' \leqq h - \frac{h - 1}{q}.$$

Therefore,

$$q\delta' - 1 \leqq qh - h + 1 - 1 = (q - 1)h,$$

or

$$\nu'(q-1) \geqq q\delta' - 1.$$

Comparing this with (5), only equality is possible; i.e.,

$$q\delta' - 1 = (q-1)h.$$

This implies that $(h-1)/q$ is an integer, and

$$\delta' = h - \frac{h-1}{q} = \frac{\delta}{q}.$$

$C(S')$ is thus a set of points with

$$\nu' = h, \qquad \delta' = \frac{\delta}{q} \qquad \text{and} \qquad (q-1)\nu' = q\delta' - 1.$$

Since $q^{r-3} < \delta/q \leqq q^{r-2}$ we can apply the induction hypothesis, which gives us

$$\delta' = q^{r-2}, \qquad \nu' = 1 + q + \cdots + q^{r-2}$$

or

$$\delta = q\delta' = q^{r-1}, \qquad \nu = q\nu' + 1 = 1 + q + \cdots + q^{r-1}$$

and the points $C(S')$ are all the points of a linear space B_{r-2} in H_{k-2}.

We can always find in H_{k-2} a $(k-3)$-dimensional subspace, say D_{k-3}, which intersects B_{r-2} in a space of dimension $(r-3)$, and thus contains exactly

$$1 + q + \cdots + q^{r-3} = \frac{h-1}{q} = \bar{\alpha}$$

points of $C(S)$.

Consider the hyperplanes of $T_{k-1}(q)$ which pass through D_{k-3}. From (8), we have for these

$$\beta_i = \bar{\beta} = h - \frac{h-1}{q},$$

so that the total number of points of $C(S)$ in each hyperplane is

$$\bar{\alpha} + \bar{\beta} = h.$$

By the previous argument the intersection of $C(S)$ with each hyperplane is a linear space of dimension $(r-2)$. These spaces have in common a linear space of dimension $(r-3)$, the intersection of B_{r-2} and D_{k-3}. Hence the set of all their points is a linear space of dimension $(r-1)$. This proves the theorem.

We will now summarize the results of the last section. For $q = 2$, the alphabets $\mathfrak{A}_0, \mathfrak{A}_1, \cdots, \mathfrak{A}_{k-1}$ introduced at the beginning of the section are the only alphabets which attain the bound of Theorem 5. For $q > 2$ these alphabets attain this bound, and have the further property that any k-dimensional alphabet obtained from them by removing up to $(q - 2)$ arbitrary columns of the generator matrix ($q - 1$ for $\mathfrak{A}_0$) also attains this bound. They are the only alphabets with this property. Clearly the alphabets $\mathfrak{A}_0, \mathfrak{A}_1, \cdots, \mathfrak{A}_{k-1}$ are completely determined, up to equivalence, by the values of the parameters k,d,n. For a given k, d and n are restricted to a certain set of values defined at the beginning of this section.

VI. ACKNOWLEDGMENTS

The author would like to thank D. Slepian and J. B. Kruskal of Bell Telephone Laboratories and Professor A. J. Gleason of Harvard University for their careful and critical reading of the manuscript and for several suggestions which resulted in substantial improvements throughout. Previous work in the field of nonbinary error correction, not referred to in the paper, is described in Refs. 7 through 10.

APPENDIX

Slepian's Error-Correction Procedure

Let $F(q)$ denote a finite field, and $G_n(q)$ the group, of order q^n, of all possible rows of n symbols picked from $F(q)$. The group operation is place-by-place addition under the rules prevailing in $F(q)$. Let A be a subgroup of G_n. [For the present purposes A need not be a vector space over $F(q)$; the two concepts are the same if and only if $F(q)$ is a prime field.]

Partition G_n into cosets with respect to A, with an element of least weight in each coset being picked as "coset leader." The element (00 $\cdots$ 0) is, of course, the coset leader of A itself. The cosets are formed into a table as illustrated in Table III. The group A is the first row of the coset table. The first column of the table contains the coset leaders. In the case of Table III these are, besides (0000), all the elements of weight 1 in $G_3(3)$.

The element in the sth row and the tth column of the coset table is obtained by adding the sth coset leader to the element (of A) in the first row and the tth column. The sth row is exactly the coset determined by the sth coset leader, and every element of $G_n(q)$ appears exactly once in the table.

TABLE III — COSETS WITH RESPECT TO A FOR $G_n(q) = G_3(3)$

	1	2	3	4	5	6	7	8	9
1	0000	1011	0112	1120	1202	2022	0221	2210	2101
2	1000	2011	1112	2120	2202	0022	1221	0210	0101
3	2000	0011	2112	0120	0202	1022	2221	1210	1101
4	0100	1111	0212	1220	1002	2122	0021	2010	2201
5	0200	1211	0012	1020	1102	2222	0121	2110	2001
6	0010	1021	0122	1100	1212	2002	0201	2220	2111
7	0020	1001	0102	1110	1222	2012	0211	2200	2121
8	0001	1012	0110	1121	1200	2020	0222	2211	2102
9	0002	1010	0111	1122	1201	2021	0220	2212	2100

The error-correction procedure is as follows: If the received element is a letter of A it is accepted as correct. If not, it is located in the coset table, say in row s, column t, and the letter of A in row 1, column t is substituted.

It is clear that the example of Table III will correct all single errors. Column 2 contains, besides (1011) which belongs to A, all the elements of $G_3(3)$ which differ from (1011) in exactly one place.

In general, if it is required to correct all single, double, etc., errors it is necessary that all elements of $G_n(q)$ of weights 1, 2, etc., appear as coset leaders in the coset table formed by A. Let d be the minimum weight of the letters of A, other than zero. The coset formed by a leader of weight 1 will consist of elements of weight at least $(d - 1)$. Hence all elements of $G_n(q)$ of weight 1 appear as coset leaders if and only if $d \geqq 3$. Similarly, all elements of weight 2 appear as coset leaders if and only if $d \geqq 5$. If it is required to correct all e-fold errors, the alphabet A must have $d \geqq 2e + 1$.

REFERENCES

1. Hamming, R. W., Error Detecting and Error Correcting Codes, B.S.T.J., **29**, 1950, p. 147.
2. Slepian, D., A Class of Binary Signaling Alphabets, B.S.T.J., **35**, 1956, p. 203.
3. Bose, R. C. and Kuebler, R. R., Jr., A Geometry of Binary Sequences Associated with Group Alphabets in Information Theory, Ann. Math. Stat., **31**, 1960, p. 113.
4. Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.
5. van der Waerden, B. L., *Modern Algebra*, Vol. 1, Ungar, New York, 1949.
6. McClusky, E. J., Jr., Error-Correcting Codes — A Linear Programming Approach, B.S.T.J., **38**, 1959, p. 1485.
7. Zaremba, S. K., Covering Problems Concerning Abelian Croups, J. Lond. Math. Soc., **27**, 1952, p. 242.
8. Ulrich, W., Non-Binary Error Correction Codes, B.S.T.J., **36**, 1957, p. 1341.
9. Golay, M. J. E., Notes on the Penny-Weighing Problem, Lossless Symbol Coding with Nonprimes, I.R.E. Trans., **IT-4**, 1958, p. 103.
10. Cocke, J., Lossless Symbol Coding with Nonprimes, I.R.E. Trans., **IT-5**, 1959, p. 33.